R365. Governor, Planning and Budget, Chief Information Officer.
R365-5. State Privacy Policy and Agency Privacy Policies.
R365-5-1. Purpose.
The purpose of this rule is to:
(1) establish a statewide policy for informing the public how personally identifiable information is collected and used by the State of Utah (State) websites;
(2) describe the relationships that exist between State agency privacy policies and the Privacy Policy Statement for State of Utah Websites (the State Policy);
(3) establish notification and posting requirements for State websites.

R365-5-2. Application.
All executive branch agencies of State government shall comply with this rule, except the State Board of Education, the Board of Regents and institutions of higher education, regardless of whether the State agency implements the State Policy or issues a website privacy policy of its own.

R365-5-3. Authority.
This rule is issued by the Chief Information Officer (CIO) under the authority of Section 63D-1-301.5 of the Information Technology Act, and in accordance with Section 63-46a-3 of the Utah Rulemaking Act, Utah Code Annotated.

R365-5-4. Definitions.
As used in this rule:
(1) "Conspicuous" means any material displayed, for example, in a manner that a reasonable person should notice it.
(2) "Link" means a connection marker on a Web page that permits an Internet user to gain access to one web page from another.
(3) "Home page" means the main, or first page retrieved when accessing an Internet Web site. It serves as a table of contents to the rest of the pages on the site or to other Web sites. This may refer to either a department home page or to other state agency pages such as those of an office or division.
(4) "Personally identifiable information" means any information collected online that could serve to identify an individual, including:
(a) first and last name;
(b) physical address;
(c) e-mail address;
(d) telephone number;
(e) Social Security number;
(f) credit card information;
(g) bank account information; and
(h) any combination of personal information that could be used to determine identity.
(5) "Privacy policy" means a policy or statement that describes how information collected is gathered, used, stored, retrieved, and protected.
(6) "State agency" means any agency or administrative sub-unit of the executive branch of the State government, except:

(a) the State Board of Education; and

(b) the Board of Regents and institutions of higher education.

(7) "State function" means an activity explicitly, or implicitly assigned by the legislature, as having a specific role in the operation of the state's government.

(8) "Privacy Policy Statement For State of Utah Websites" means a statement approved by the Chief Information Officer and published on the state home page http://www.utah.gov that describes to Website users the state's privacy policy as established through this rule.

(9) "Privacy Risk Assessment" means a series of questions approved by the Chief Information Officer that are designed to:

(a) assist agencies in identifying and reducing potential levels of risk to the privacy of individuals using an online government service through state of Utah Websites;

(b) provide information to assist in determining different levels of security;

(c) collect information needed to determine, and if necessary, create an agency privacy policy if one is needed in addition to the State Policy.

(10) "Website" means a set of documents or pages located on the World Wide Web.

R365-5-5. Agency Privacy Policies.

(1) A State agency may issue a privacy policy that provides additional detail to, but does not conflict with the terms of this rule.

(2) When a State agency is required by a federal statute, federal regulation, or State statute to collect or use the personally identifiable information of those accessing its website in a manner that is inconsistent with this rule, it shall issue a privacy policy of its own.

(3) An agency privacy policy issued in accordance with this rule shall apply only to the website of the issuing State agency.

(4) An agency may not substitute its own privacy policy for this rule, unless a state law, federal regulation or federal statute requires an agency to treat personally identifiable information in a way that is inconsistent with this rule. In this case, the specific provision or provisions of this rule that conflict with the state statute, federal regulation or federal statute does not apply. If that occurs, the remainder of the provisions of this rule shall apply to the agency.

R365-5-6. Use of Personally Identifiable Information.

(1) Any personally identifiable information an individual provides to a State website shall be used solely by the State, its entities, and third party agents with whom it has contracted to perform a state function on its behalf, unless:

(a) this rule is superceded by a federal statute, federal regulation, or State statute in which case the personally identifiable information shall be used by other parties only to the extent required by the superseding federal statute, federal regulation or State Statute, or

(b) the information is designated as public record by an individual State agency as authorized under Title 63, Chapter 2 of the Utah Code, Government Records Access and Management Act.

R365-5-7. Notification and Posting Requirements.

(1) If either of the exceptions listed in R365-5-7 Subsection (1)(a) or (b) apply or if the State agency issues an agency privacy policy for its website as permitted under this rule, then the agency shall conspicuously post that information on the Web pages where personally identifiable information is collected or on the home page of its Website including the following:

(a) a notice that such personally identifiable information is subject to public access, if such information is public record;

(b) a notice and a summary or link to the citation of any State statute, federal statute, or federal regulation that supercedes part or all of this rule;

(c) a link to the agency's privacy policy;

(d) a link from the agency's website to this rule and

(e) a link from the agency's website to the State Policy.

(2) The agency privacy policy shall indicate:

(a) the name of the issuing agency;

(b) a statement that the agency privacy policy applies to its own website only;

(c) a statement about what personally identifiable information the policy specifically applies to; and

(d) a statement defining how its agency privacy policy differs from this rule.

(3) The effective date for this subsection shall be four months from the effective date of this rule for information collected through existing online applications. If requested in writing by the agency, an additional extension for up to 30-days may be given by the chief information officer. For all new online applications the conditions of this subsection must be met prior to the application going "live."

R365-5-8. Privacy Risk Assessment for Online Applications.

Each state agency shall complete a "Privacy Risk Assessment" that is authorized by the CIO, for all online applications. The agency shall maintain a copy of each completed assessment for a period of four years for the purpose of providing audit documentation.

R365-5-9. Periodic Audits.

The CIO may measure compliance of a State agency and its employees with this rule by conducting periodic audits in accordance with Section 63D-1-301.5, Utah Code Annotated. In performing audits, the CIO may utilize external auditors, an agency's internal auditor(s) or both.

R365-5-10. Statutes that may affect this Rule.

Included among the federal and State statutes that may supersede portions of this rule are the Driver's Privacy Protection Act of 1994, Title 18, Section 2721, United States Code; and Sections 41-1a-116, 53-1-104, 53-1-109, and 59-1-403, Utah Code Annotated.

KEY: privacy, website, CIO
2001
63D-1-301.5

63-46a-3
63-2-101 et seq.

Non-substantive change

R365-5-7. Notification and Posting Requirements.
(1) If either of the exceptions listed in R365-5-6